



IFW

PTO/SB/21 (08-03)
Approved for use through 08/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TRANSMITTAL
FORM**

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

3

Application Number	10/708,949
Filing Date	04/02/2004
First Named Inventor	Chen-Huang FAN
Art Unit	
Examiner Name	
Attorney Docket Number	ACMP0048USA

ENCLOSURES (Check all that apply)

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> Fee Transmittal Form
<input type="checkbox"/> Fee Attached
<input type="checkbox"/> Amendment/Reply
<input type="checkbox"/> After Final
<input type="checkbox"/> Affidavits/declaration(s)
<input type="checkbox"/> Extension of Time Request
<input type="checkbox"/> Express Abandonment Request
<input type="checkbox"/> Information Disclosure Statement
<input checked="" type="checkbox"/> Certified Copy of Priority Document(s)
<input type="checkbox"/> Response to Missing Parts/ Incomplete Application
<input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53 | <input type="checkbox"/> Drawing(s)
<input type="checkbox"/> Licensing-related Papers
<input type="checkbox"/> Petition
<input type="checkbox"/> Petition to Convert to a Provisional Application
<input type="checkbox"/> Power of Attorney, Revocation
Change of Correspondence Address
<input type="checkbox"/> Terminal Disclaimer
<input type="checkbox"/> Request for Refund
<input type="checkbox"/> CD, Number of CD(s) _____ | <input type="checkbox"/> After Allowance communication to Technology Center (TC)
<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Status Letter
<input type="checkbox"/> Other Enclosure(s) (please identify below): |
|--|---|--|

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Winston Hsu, Reg. No.: 41,526
Signature	<i>Winston Hsu</i>
Date	6/24/2004

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

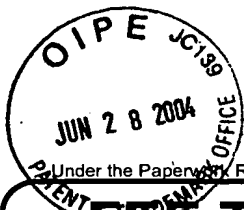
Typed or printed name

Signature

Date

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT (\$) 0.00

Complete if Known

Application Number	10/708,949
Filing Date	04/02/2004
First Named Inventor	Chen-Huang FAN
Examiner Name	
Art Unit	
Attorney Docket No.	ACMP0048USA

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 50-3105
Deposit Account Name: North America Intellectual Property Corp.

The Director is authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☐ Credit any overpayments

☒ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	
SUBTOTAL (1)				(\$) 0.00	

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

Extra Claims Fee from below Fee Paid
Total Claims -20** = X =
Independent Claims -3** = X =
Multiple Dependent =

Large Entity		Small Entity		Fee Description
Fee Code	Fee (\$)	Fee Code	Fee (\$)	
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) (\$) 0.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee (\$)	Fee Code	Fee (\$)		
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for ex parte reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$) 0.00

SUBMITTED BY

Name (Print/Type) Winston Hsu

Registration No. 41,526
(Attorney/Agent)

(Complete (if applicable))

Telephone 886289237350

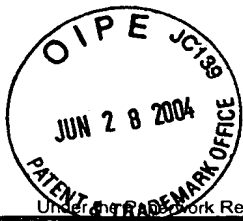
Signature

Date

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



PTO/SB/02B (11-00)

Approved for use through 10/31/2002. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

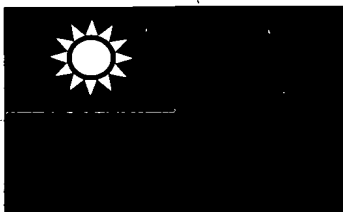
DECLARATION — Supplemental Priority Data Sheet

Additional foreign applications:

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
092107825	Taiwan R.O.C	04/04/2003	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

ACH-48



中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下：

This is to certify that annexed is a true copy from the records of this
office of the application as originally filed which is identified hereunder:

申請日：西元 2003 年 04 月 04 日
Application Date

申請案號：092107825
Application No.

申請人：明基電通股份有限公司
Applicant(s)

局長
Director General

蔡練生

發文日期：西元 2003 年 5 月 14 日
Issue Date

發文字號：09220483040
Serial No.

申請日期：	IPC分類
申請案號：	

(以上各欄由本局填註)

發明專利說明書

一、 發明名稱	中 文	以防寫解密金鑰防止手機加密網路鎖被破解之保護方法及相關裝置
	英 文	Network Lock Method And Related Apparatus By CIPHERED Network Lock And Inerasable Deciphering Key

二、 發明人 (共3人)	姓 名 (中文)	1. 范振煌 2. 杜本權
	姓 名 (英文)	1. Fan, Chen-Huang 2. Du, Ben-Chuan
	國 籍 (中英文)	1. 中華民國 TW 2. 中華民國 TW
	住居所 (中 文)	1. 苗栗縣頭份鎮尖豐路五十二號 2. 台北縣新店市三民路七十五巷九弄十二號二樓
	住居所 (英 文)	1. No. 52, Jian-Feng Rd., Tou-Fen Town, Miao-Li Hsien, Taiwan, R.O.C. 2. 2F, No.12, Alley 9, Lane 75, San-Min Rd., Hsin-Tien City, Taipei Hsien, Taiwan, R.O.C.

三、 申請人 (共1人)	名稱或 姓 名 (中文)	1. 明基電通股份有限公司
	名稱或 姓 名 (英文)	1. BenQ Corporation
	國 籍 (中英文)	1. 中華民國 TW
	住居所 (營業所) (中 文)	1. 桃園縣龜山鄉山鶯路157號 (本地址與前向貴局申請者相同)
	住居所 (營業所) (英 文)	1. No.157, Shan-Ying Road, Kweishan, Tao-Yuan Hsien, Taiwan, R.O.C.
	代表人 (中文)	1. 李焜耀
	代表人 (英文)	1. Lee, Kuen-Yao



申請日期：	IPC分類
申請案號：	

(以上各欄由本局填註)

發明專利說明書

發明名稱	中文	
	英文	
發明人 (共3人)	姓名 (中文)	3. 程意雯
	姓名 (英文)	3. Cheng, Yi-Wen
	國籍 (中英文)	3. 中華民國 TW
	住居所 (中文)	3. 台北市光復南路十三巷四十三號二樓
	住居所 (英文)	3. 2F, No. 43, Lane 13, Kuang-Fu S. Rd., Taipei City, Taiwan, R.O.C.
申請人 (共1人)	名稱或姓名 (中文)	
	名稱或姓名 (英文)	
	國籍 (中英文)	
	住居所 (營業所) (中文)	
	住居所 (營業所) (英文)	
	代表人 (中文)	
	代表人 (英文)	



四、中文發明摘要 (發明名稱：以防寫解密金鑰防止手機加密網路鎖被破解之保護方法及相關裝置)

本發明提供一種無線通信網路之網路鎖保護方法及相關裝置。該方法係將不同的手機對應於一非對稱密碼演算法之相異加密金鑰及解密金鑰；對應一手機網路鎖之存取資料內容會根據對應之加密金鑰以一非對稱密碼演算法加密後儲存於該手機中，而解密所用之解密金鑰則儲存於該手機的防寫記憶體中，使該解密金鑰不會被覆寫；而該明文存取資料及該加密金鑰則僅記錄於該無線通信網路之服務提供端中。要實施網路鎖時，該手機會以防寫記憶體中之解密金鑰將加密之存取資料內容解密以驗證該手機是否能存取該無線通信網路之通信服務。

伍、(一)、本案代表圖為：第3圖

(二)、本案代表圖之元件代表符號簡單說明：

30

通信網路

32A-32B 手機

六、英文發明摘要 (發明名稱：Network Lock Method And Related Apparatus By Ciphered Network Lock And Inerasable Deciphering Key)

A protection method and related apparatus for network lock of a communication network. The method includes: associating different cell phones to different enciphering and deciphering keys of an asymmetric encryption algorithm. An access information of a network lock corresponding to a cell phone is enciphered by the corresponding enciphering key. Then the

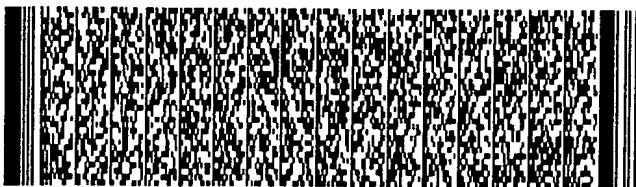


四、中文發明摘要 (發明名稱：以防寫解密金鑰防止手機加密網路鎖被破解之保護方法及相關裝置)

36	處理器	50A-50B	防寫記憶體
40A-40B	資料記憶體	52	資料庫
54	密碼演算法	IDA-IDB	裝置識別碼
EKA-EKB	加密金鑰	DKA-DKB	解密金鑰
PTA-PTB、PTA2			明文存取資料
CTA-CTB	密文存取資料		

六、英文發明摘要 (發明名稱：Network Lock Method And Related Apparatus By CIPHERED Network Lock And Inerasable Deciphering Key)

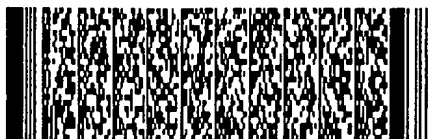
enciphered network lock is stored in the cell phone, and the corresponding deciphering key is recorded in an inerasable memory of the cell phone. The original plaintext access information of the network lock and the enciphering key is stored only in a service provider of the communication network. When the cell phone tries to access the communication network, it



四、中文發明摘要 (發明名稱：以防寫解密金鑰防止手機加密網路鎖被破解之保護方法及相關裝置)

六、英文發明摘要 (發明名稱：Network Lock Method And Related Apparatus By Ciphred Network Lock And Inerasable Deciphering Key)

deciphered the enciphered network lock using the deciphering key stored in the inerasable memory to verify the network lock of the cell phone.



一、本案已向

國家(地區)申請專利

申請日期

案號

主張專利法第二十四條第一項優先權

無

二、☐主張專利法第二十五條之一第一項優先權：

申請案號：

無

日期：

三、主張本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間

日期：

四、☐有關微生物已寄存於國外：

寄存國家：

寄存機構：

寄存日期：

寄存號碼：

無

☐有關微生物已寄存於國內(本局所指定之寄存機構)：

寄存機構：

寄存日期：

寄存號碼：

無

☐熟習該項技術者易於獲得, 不須寄存。



五、發明說明 (1)

發明所屬之技術領域

本發明係提供一種網路鎖保護方法及相關裝置，尤指一種將解密金鑰儲存於手機中之防寫記憶體、並以該解密金鑰將加密後之網路鎖資料內容解密以驗證網路鎖機制之網路鎖保護方法及相關裝置。

先前技術

在資訊發達的現代社會中，便利的無線通信網路已為人類交流、資訊交換最重要的途徑之一。只要以方便輕巧、操作簡便的手機，人人都能輕易地利用無線通信網路中的通信服務，隨時隨地享受無遠弗屆的資訊存取能力。為了使通信網路能永續經營，提高通信服務之品質，如何維持通信網路中的通信秩序，並確保通信網路中用戶的權益，也就成了現代資訊業界研發的重點之一。

一般來說，無線通信網路中的通信服務是由網路服務端提供的，手機的使用者則付費成為網路服務端的合用用戶，並得以使用網路服務端提供的通信服務。為了要確保合法用戶的權益，當手機的使用者要以手機來存取通信服務時，手機會透過一網路鎖機制驗證使用者是否為合法之用戶；若使用者並非合法用戶，手機本身就

五、發明說明 (2)

會限制使用者對通信網路的存取。關於此情形，請參考圖一。圖一為一習知通信系統10中，各通信裝置（如手機12、13）與一服務提供端28配置的示意圖。以手機12做為代表來說明習知通信系統10之通信裝置，手機12中設有一無線電訊號之收發模組14、一主控手機運作的處理器16、一用來記錄資料的資料記憶體20（譬如說是快閃記憶體等非揮發性記憶體）、一用來識別用戶身份的用户識別卡24、一用來將聲波轉換為電子訊號的麥克風18A、一揚聲器18B以及人機介面21。人機介面21可包含鍵盤、顯示器、振動器等等，讓手機12的使用者得以透過人機介面21操控手機12，並由人機介面21得知手機12運作的情形。服務提供端28則設有收發傳輸無線電訊號的基地台29，以在各手機間傳輸無線電訊號，提供通信服務。舉例來說，手機12使用者的語音聲波可由麥克風18A接收並轉為電子訊號，由處理器16將其適當地編碼（encoding），再傳輸到收發模組14中進一步調變為射頻訊號，由收發模組14以無線電形式發射至基地台29。基地台29接收手機12發出之無線電訊號後，就可將此訊號再透過基地台29以無線電的方式傳輸至手機13，讓手機13的使用者可接收到手機12使用者傳來的訊息。同理，手機13要傳輸至手機12的語音訊息，也會以無線電方式透過基地台29的轉接傳輸至手機12，由手機12的收發模組14接收並解調為基頻訊號，再由處理器16適當地解碼（decoding），傳輸至揚聲器18B，轉換成聲波語音播放出

五、發明說明 (3)

來，讓手機 12 的使用者能夠聽到。如此一來，手機 12、13 之使用者就能透過服務提供端 28 提供的通信服務相互溝通。

然而，正如前述，為了維護通信網路 10 合法用戶的正當權利，在手機 12 要存取通信網路 10 的通信服務前，手機 12 還會自動進行一驗證步驟，以驗證手機 12 的使用者是否能合法存取通信網路 10 的通信服務。為了配合此一驗證步驟的進行，手機 12 中的用戶識別卡（即所謂的 SIM 卡）24 記錄有一用戶識別碼 26，用來代表手機 12 使用的身份。一般來說，用戶識別卡 24 是以可插拔的方式安裝於手機 12 中；當一使用者要使用手機 12 來存取通信網路 10 時，就要將其持有的用戶識別卡 24 插入安裝於手機 12 中，讓手機 12 可辨識使用者的身份。對應於用戶識別卡 24 中的用戶識別碼 26，資料記憶體 20 中除了記錄手機 12 運作所必需的資料外（像是手機 12 的韌體），也記錄有一裝置識別碼 23，及用來進行驗證步驟的存取資料 22。其中裝置識別碼 23 為各手機獨有的專屬識別碼（像是 IMEI 識別碼，International Mobile Equipment Identity）；換句話說，不同的手機，其所具有的裝置識別碼也不同。而存取資料 22 即用來記錄手機 12 網路鎖的狀態。所謂的網路鎖，就是用來定義手機 12 是否僅能接受某些用戶識別碼來存取通信網路 10 的通信服務。而存取資料 22 中，即記錄了網路鎖是否啟動，以及手機 12

五、發明說明 (4)

可接受之合法用戶識別碼。舉例來說，當用戶識別碼 26 中某些欄位之值在某一預設範圍中時，手機 12 可接受其為合法之用戶識別碼；而該預設範圍即記錄於存取資料 22 中。在習知技術中，當手機 12 要進行驗證步驟時，處理器 16 會由資料記憶體 20 中讀取存取資料 22，根據存取資料 22 來判斷手機 12 的網路鎖是否啟動。若存取資料 22 中記錄網路鎖是啟動的，處理器 16 會進一步檢查用戶識別卡 24 中的用戶識別碼 26 是否在存取資料 22 記錄之合法用戶識別碼中。若用戶識別碼 26 符合合法用戶識別碼（舉例來說，承前所述，用戶識別碼 26 中某些欄位之值在存取資料 22 記錄之預設範圍中），處理器 16 就會判斷用戶識別卡 24 的持有者為通信網路 10 的合法使用者，並使手機 12 能繼續進行後續的步驟，讓手機 12 的使用者（也就是用戶識別碼 24 的持有者）能透過手機 12 存取通信網路 10 的通信服務。反之，若處理器 16 比對發現用戶識別卡 24 中的用戶識別碼 26 並不在存取資料 22 記錄之合法用戶識別碼範圍之內，處理器 16 就會判斷用戶識別卡 24 之持有者並非通信網路 10 的合法使用者，並使手機 12 停止對通信網路 10 的存取。另一方面，若進行驗證步驟時處理器 16 發現存取資料 22 中記錄網路鎖並沒有啟動，處理器 16 就不會檢查用戶識別碼 26，而直接允許用戶識別卡 24 之持有者透過手機 12 存取通信網路 10 之通信服務。

五、發明說明 (5)

簡而言之，上述之習知網路鎖的實現方式，即是依靠資料記憶體 20 中儲存的存取資料 22 來判斷用戶識別卡 24 的持有者是否能透過手機 12 存取通信網路 10 的通信服務。然而，此種習知的方法也隱含了網路鎖被非法使用者破解的危機。舉例來說，當一非法使用者要破解手機 12 的網路鎖時，非法使用者可以由網路鎖沒有被啟動的其他手機中取得其存取資料；由於此類手機中的網路鎖沒有啟動，此存取資料中會記錄網路鎖為不啟動，而此存取資料即可做為一破解存取資料。即使手機 12 的存取資料 22 中記錄手機 12 的網路鎖為啟動，但非法使用者可破解存取資料覆寫至資料記憶體 20 中，將原來的存取資料 22 覆蓋 (overwrite)，以此破解存取資料來取代原來的存取資料 22。等到手機 12 要進行驗證步驟時，就會錯誤地根據破解存取資料而不啟動網路鎖，而手機 12 的網路鎖也就被破解了。此時即使用戶識別卡 24 上的用戶識別碼 26 並非合法用戶識別碼，用戶識別碼 24 的持有者也可非法地以手機 12 來存取通信網路 10 的通信服務。在技術層面上，為了方便對手機 12 的維修、測試，手機 12 中的資料記憶體 20 會設有維修用的預設接點，而非法使用者就可利用這些預設接點以特殊的資料燒錄工具（像是 TAG tool）將破解存取資料寫入至資料記憶體 20 並覆蓋原來的存取資料 22，以破解手機 12 的網路鎖。尤有甚者，非法使用者還能直接改寫存取資料 22 中的記錄，譬如說將存取資料 22 中原本記錄為啟動的網路鎖改為不啟

五、發明說明 (6)

動，也能破解手機 12 的網路鎖。另外，非法使用者還能刪除存取資料 22。一般來說，在習知之手機 12 中，當處理器 16 發現資料記憶體 20 中沒有存取資料 22 時，會根據一預設的存取資料來進行網路鎖之驗證步驟，而此預設存取資料多半不會啟動網路鎖之功能。這樣一來，非法使用者也能破解手機 12 的網路鎖。一旦網路鎖被非法破解，就會影響通信網路 10 的通信秩序，損及服務提供端及各合法用戶（合法用戶識別卡之持有者）的權益。

發明內容

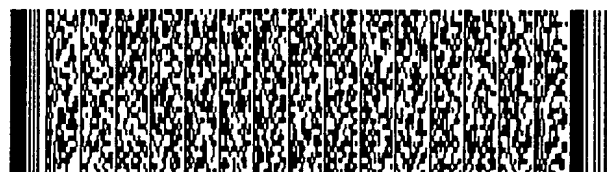
因此，本發明之主要目的，即在於提供一種安全性較高的網路鎖保護機制及相關系統、裝置，以克服習知網路鎖機制易遭破解的缺點。

在習知的網路鎖機制中，手機中的處理器是依據資料記憶體中存取資料所記錄之網路鎖狀態來進行網路鎖的驗證步驟；一旦存取資料被覆寫、竄改，網路鎖就會被破解，影響通信網路中的正常秩序及各方的合法權益。

在本發明中，係以一非對稱性的密碼演算法，針對不同的手機以不同的加密金鑰將各手機網路鎖之存取資料加密為密文存取資料，各手機中僅儲存密文存取資

五、發明說明 (7)

料，並以一防寫記憶體記錄解密之對應解密金鑰；而各手機對應的加密金鑰則僅保留於服務提供端之資料庫中。其中該防寫記憶體為一單次寫入 (OTP, One-Time Programmable) 記憶體或為一快閃記憶體之可鎖定 (lockable) 記憶區，以使記錄於其中的解密金鑰不會被覆寫。當一手機要進行驗證步驟時，該手機會根據該防寫記憶體中的解密金鑰將資料記憶體中的密文存取資料解密為明文存取資料，並根據明文存取資料中記錄的網路鎖狀態來進行相關之網路鎖驗證。由於各手機對應的加解密金鑰皆互不相同，且各手機中的解密金鑰無法被寫，即使非法使用者意圖破解某一手機 A 之網路鎖而將另一手機 B 中記錄的密文存取資料覆寫至手機 A 中，但當手機 A 進行驗證步驟而將該密文存取資料解密時，會因為手機 A、B 之解密金鑰不同而使手機 A 無法解出正確格式的明文存取資料，此時手機 A 即可判斷網路鎖已遭破壞，可以停止對通信網路的存取，以防止通信網路之正常秩序受不法侵害。由於各手機中儲存的存取資料為密文之存取資料，也可防止非法使用者以直接修改存取資料的方式來破解網路鎖。由於加密金鑰並不會暴露於各手機或通信網路中，即使非法使用者能竄改明文存取資料，也無法以正確的加密金鑰將竄改後之明文存取資料加密為對應解密金鑰的正確密文存取資料。另外，當服務提供端要更新一手機中的網路鎖存取資料時，可由資料庫中找出該手機對應的加密金鑰，將更新的明文存取資料加

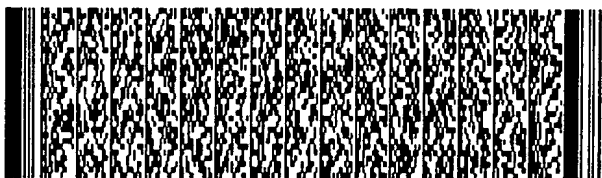


五、發明說明 (8)

密為新的密文存取資料，再將此一更新後之密文存取資料存入該手機的資料記憶體中。經由上述機制，本發明將可確保各手機中網路鎖的安全，進一步維護通信網路中的正常秩序及各方的合法權益。

實施方式

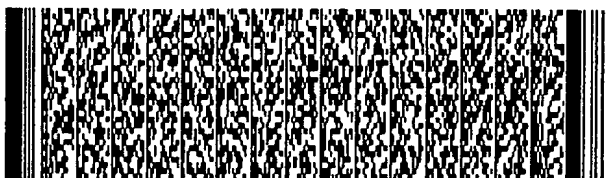
請參考圖二。圖二為本發明通信網路30配置的示意圖。通信網路30可以是一無線通信網路，以服務提供端48提供通信服務，而各使用者則透過各手機（圖二中繪兩手機32A、32B做為代表）來存取通信網路30的通信服務。以手機32A做為代表來說明通信網路30中各手機的構造；手機32A做為一通信裝置，其包括有一用來收發無線電訊號的收發模組34、一用來控制手機12運作之處理器36、一用來將聲波轉換為電子訊號的麥克風38A、一用來將電子訊號轉換為聲波的揚聲器38B、一用來以非揮發性方式儲存資料的資料記憶體40A、一非揮發性的防寫記憶體50A、一以可插拔方式安裝於手機32A中的客戶識別卡45，以及一人機介面(MMI, Man-Machine Interface)41。人機介面41可以包括有鍵盤、顯示器、用來提示來電的振動器及另一揚聲器等等，讓手機32A的使用者可透過此人機介面41操控手機32A，並由顯示器等介面得知手機32A的運作狀態。服務提供端48則設有多個基地台49，用來向各手機收發無線電訊號，以向各手機



五、發明說明 (9)

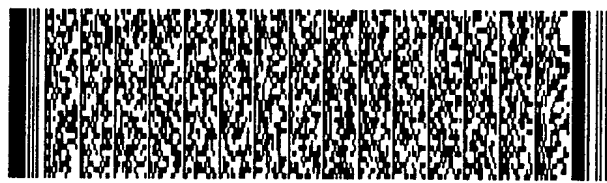
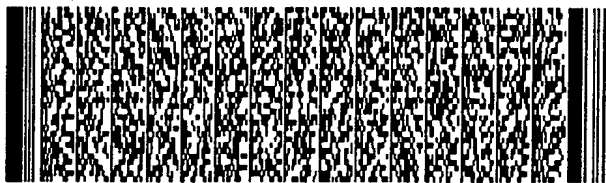
提供通信服務。舉例來說，手機 32A 使用者的語音聲波可經由麥克風 38A 接收轉為電子訊號，經由處理器 36 的編碼、訊號處理後傳輸至收發模組 34，由收發模組 34 將其調變為射頻訊號後，以無線電的方式發射至服務提供端 48 的基地台 49。服務提供端 48 在接收手機 32A 傳來的無線電訊號後，可透過另一基地台 49 將手機 32A 的訊號再以無線電方式傳輸至手機 32B，讓手機 32B 的使用者能經由服務提供端 48 的通信服務而接收到手機 32A 使用者傳來的訊息。同理，手機 32B 的訊息也能經由服務提供端 48 訊號轉接之通信服務而傳至手機 32A 的收發模組 34，由收發模組 34 將其解調為基頻訊號，再由處理器 36 進一步解碼、訊號處理，並由揚聲器 38B 將其以聲波的方式播放出來（或經由人機介面 41 顯示出來）。

不過，如前所述，為了維持通信網路 30 正常的通信秩序及各使用者的合法權益，在手機 32A 的使用者在透過手機 32A 存取通信網路 30 的通信服務前，要先在手機 32A 中插入其所持有的用戶識別卡 45，而手機 32A 就會依據用戶識別卡 45 上記錄的用戶識別碼 46 自動地進行一驗證步驟，以透過網路鎖的機制驗證手機 32A 的使用者（亦即用識別卡 45 的持有者）是否為通信網路 30 的合法用戶，並決定是否要繼續存取通信服務。為了配合本發明驗證機制的實施，在本發明通信網路 30 中，各手機的資料記憶體除了儲存代表各手機的裝置識別碼（及各手機的動



五、發明說明 (10)

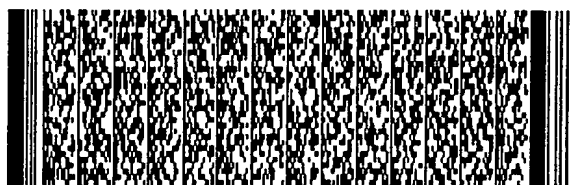
體)外,還儲存有一密文存取資料;而各手機也另設有一防寫記憶體,用來儲存一對應的解密金鑰。如圖二所示,手機32A的資料記憶體40A中即儲存有手機32A的裝置識別碼IDA及一密文存取資料CTA;而其防寫記憶體50A中則儲存有一解密金鑰DKA。基於相同的配置原理,手機32B中的資料記憶體40B則儲存有對應手機32B的裝置識別碼IDB、密文資料CTB,並於其防寫記憶體50B中儲存有一解密金鑰DKB(手機32A的基本構造與手機32A相似,在不妨礙本發明技術揭露的情形下,手機32B的部分構造,如收發模組、處理器等等已於圖二中省略未示)。如前所述,各手機對應的裝置識別碼(像是IMEI識別碼)係用來獨一無二地識別出該手機,故不同的手機也具有不同的裝置識別碼,如手機32A的裝置識別碼IDA就和手機32B的裝置識別碼IDB不同。另外,在通信網路30中,不同手機中記錄的解密金鑰、密文存取資料也互不相同。以圖二為例,各手機32A、32B對應的解密金鑰DKA、DKB以及密文存取資料CTA、CTB即互不相同。其中,各手機的解密金鑰是儲存於防寫記憶體中的。此防寫記憶體的特性即是其內記錄的資料具有唯讀的特性;一旦資料被燒錄記錄於防寫記憶體後,該資料即無法再被覆寫。在實際施時,此防寫記憶體可以是單次可程化(OTP, One-Time Programmable)記憶體;一旦資料被寫入防寫記憶體後,該資料就不能被覆寫而具有唯讀(read-only)的特性。另外,在現代的某些快閃記憶體中,已經可劃



五、發明說明 (11)

分出部分的記憶區為可鎖定(lockable)的記憶區；同樣地，資料被燒錄、寫入至此可鎖定之記憶區後，就不能再被覆寫而具有唯讀的特性。相對地，在同一快閃記憶體不具有可鎖定特性之記憶區中，資料還是可被重複寫入、抹除。利用這樣的快閃記憶體，本發明中的資料記憶體、防寫記憶體就能實施於同一快閃記憶體上，其中可鎖定之記憶區做為防寫記憶體，用來記錄各手機對應的解密金鑰；不具有可鎖定特性而可重複覆寫的記憶區，即可當作資料記憶體，以記錄手機的韌體及裝置識別碼、密文存取資料等等。

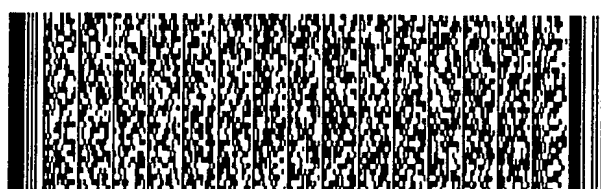
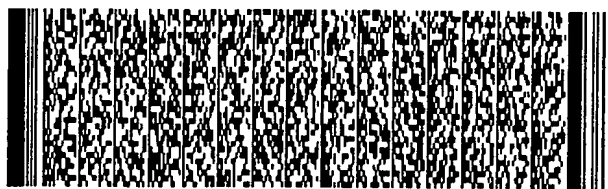
配合本發明的實施，本發明於服務提供端48也設有一資料庫52，用來記錄各手機對應之裝置識別碼、一對應之加密金鑰及一明文存取資料，也可選擇性地記錄各手機對應的解密金鑰。舉例來說，針對圖二中的兩手機32A、32B，資料庫52即記錄了手機32A的裝置識別碼IDA，並以裝置識別碼IDA為記錄的索引標的，記錄了手機32A對應之加密金鑰EKA、解密金鑰DKA及明文存取資料PTA。同理，針對手機32B，資料庫48中也以手機32B之裝置識別碼IDB做為記錄索引之標的，記錄了手機32B對應加密金鑰EKB、解密金鑰DKB以及明文存取資料PTB。其中，對應各手機的明文存取資料，就是用來記錄該手機網路鎖之存取資料內容，像是網路鎖是否啟動，網路鎖所能接受之合法用戶識別碼等等。



五、發明說明 (12)

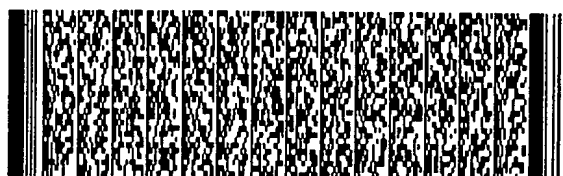
本發明網路鎖機制實施的原理可先描述如下。本發明是將各手機網路鎖的存取資料根據該手機對應之加密金鑰以非對稱之密碼演算法加密，成為該手機資料記憶體中之密文存取資料。等到該手機在存取通信服務前，要進行驗證步驟時，該手機之處理器即以防寫記憶體中的解密金鑰將密文存取資料解密為明文存取資料，再依據明文存取資料中記錄的事項（如網路鎖是否啟動，合法用戶識別碼之範圍）來比對該手機之用戶識別卡，持有者是否為合法用戶，實現網路鎖機制。至於本發明進步的實施細節，請繼續參考圖三（並併參考圖二）的示意圖。為了方便後續說明，簡化圖式，在不妨礙本發明技術揭露的情形下，圖三中手機32A、32B的部分裝置（如收發模組等等）已經省略未繪出。

承前所述，本發明在實施時會以一預設之非對稱密碼演算法將明文存取資料、密文存取資料加密為一密文，與將該密文解密為原來明文所需的一對應解密金鑰，者並不相同。換句話說，當明文以加密金鑰加密為密文後，該密文無法以同一個加密金鑰解密為原始的明文，必須要經由對應的特定解密金鑰對該明文加密所得出的



五、發明說明 (13)

結果，和以該加密金鑰對該明文加密所得出的密文，兩者也不會相同。根據此密碼演算法，本發明可預先算出複數組不同的加密金鑰及對應之解密金鑰，各組的加密金鑰均不相同。配合各手機的出廠，各手機會被賦予專屬的對應裝置識別碼，而本發明即可利用各手機的裝置識別碼做為記錄索引標的，將一組加密金鑰及對應之解密金鑰指定予一手機，並連同該手機對應的明文存取資料，一同記錄於服務提供端 48 的資料庫 52 中。如圖三中的示意例，本發明可於服務提供端 48 預先根據非對稱的密碼演算法 54 計算出加密金鑰 EKA 及其對應之解密金鑰 DKA、加密金鑰 EKB 及對應之解密金鑰 DKB 等等。其中加密金鑰 EKA、EKB 相異；再加上密碼演算法 54 的非對稱特性，事實上加解密金鑰 EKA、EKB、DKA、DKB 皆不相同。當手機 32A 出廠時，手機 32A 會被賦予其專屬之裝置識別碼 IDA；而服務提供端 48 也就可以將加密金鑰 EKA、解密金鑰 DKA 分配予手機 32A，並以手機 32A 之裝置識別碼 IDA 為記錄索引標的，將加解密金鑰 EKA、DKA 連同手機 32A 網路鎖對應之明文存取資料 PTA 一同記錄於資料庫 52 中。同理，對應於裝置識別碼為 IDB 的手機 32B，服務提供端 48 可將加解密金鑰 EKB、DKB 分配予手機 32B；並在資料庫 52 中，將加解密金鑰 EKB、DKB 連同手機 32B 網路鎖對應之明文存取資料 PTB，一同記錄於裝置識別碼 IDB 對應之項目下。



五、發明說明 (14)

在服務提供端 48 中，除了在各手機出廠時將不同組的加解密金鑰分配給各手機，也會將各手機對應之解密金鑰寫入至該手機的防寫記憶體中。等手機出廠後而為各使用者使用時，各手機中記錄的解密金鑰也就不能被覆寫了。如圖三所示，手機 32A 的對應解密金鑰 DKA 會被記錄於防寫記憶體 50A 中，並具有不可覆寫的唯讀特性。同樣地，手機 32B 中的防寫記憶體 50B 中也以唯讀特性記錄了手機 32B 對應的解密金鑰 DKB。另外，在資料庫 52 的各筆明文存取資料，就以明文記錄了各對應手機的網路鎖狀態。然而，在本發明中，各手機網路鎖之明文存取資料並不會直接儲存於各手機中，而是會由服務提供端 48 根據各手機對應之加密金鑰以密碼演算法 54 加密為密文存取資料，再將此密文存取資料寫入至對應手機的資料記憶體 32A 中。如圖三中，各手機 32A、32B 對應之明文存取資料 PTA、PTB，即分別用來以明文記錄對應手機網路鎖之狀態。舉例來說，明文存取資料 PTA 記錄了手機 32A 的網路鎖功能是否啟動等等相關訊息。不過，如前所述，服務提供端 48 會先根據手機 32A 之加密金鑰 EKA，以密碼演算法 54 將手機 32A 之明文存取資料 PTA 加密為密文存取資料 CTA，再將密文存取資料 CTA 記錄於手機 32A 的資料記憶體 40A 中。同理，服務提供端 48 也會根據手機 32B 對應之加密金鑰 EKB，以密碼演算法 54 將手機 32B 對應之明文存取資料 PTB 加密為對應的密文存取資料 CTB，再將密文存取資料 CTB 寫入至手機 32B 的資料記憶體 40B 中。



五、發明說明 (15)

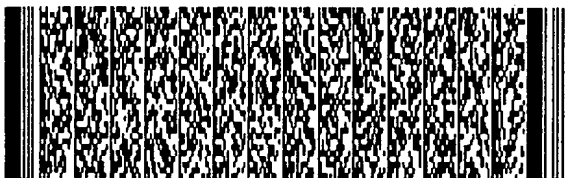
總結以上描述，在手機 32A 出廠時，資料庫 52 中已經記錄有手機 32A 對應的加解密金鑰 EKA、DKA 及網路鎖的明文存取資料 PTA；手機 32A 中也已經於防寫記憶體 50A 中以唯讀、不可覆寫之特性記錄有手機 32A 的解密金鑰 DKA，並於資料記憶體 40A 中記錄有密文存取資料 CTA。同理，在手機 32B 出廠而能為使用者使用時，手機 32B 中的防寫記憶體 50B 也以唯讀特性記錄了手機 32B 的解密金鑰 DKB，手機 32B 的資料記憶體 40B 中也記錄有手機 32B 的密文存取資料 CTB。請注意，在本發明的架構下，各手機雖有各自對應的加密金鑰及網路鎖明文存取資料，但這些資料均僅記錄於服務提供端 48 的資料庫 52 中，不會暴露於各手機中；而各手機中僅保存有對應的密文存取資料及解密金鑰。

簡而言之，在本發明架構下，當各手機出廠而能為各使用者使用時，各手機中已經儲存有該手機對應的解密金鑰及密文存取資料。如前所述，當使用者要使用手機來存取通信網路 30 之服務時，各手機要先自動進行網路鎖機制的驗證步驟，以驗證使用者是否為合法使用者。在本發明架構下，此時各手機的處理器就會由該手機中的防寫記憶體將解密金鑰讀出，以根據密碼演算法 54 來將資料記憶體中的密文存取資料解密為明文存取資料，再根據明文存取資料中記錄的網路鎖狀態來驗證使用者是否為合法的使用者。舉例來說，如圖三所示，當



五、發明說明 (16)

手機 32A 要進行驗證步驟時，手機 32A 的處理器 36 就會由資料記憶體 40A、防寫記憶體 50A 中分別將密文存取資料 CTA、解密金鑰 DKA 讀出，再利用密碼演算法 54，根據解密金鑰 DKA 將密文存取資料 CTA 解密為一明文存取資料 PTA2。由於密文存取資料 CTA 是由服務提供端 49 將明文存取資料 PTA 以手機 32A 之對應加密金鑰 EKA 加密而得，而防寫記憶體 50A 中的解密金鑰 DKA 即對應於加密金鑰 EKA，所以手機 32A 由處理器 36 解密出來的明文存取資料 PTA2，應該就等於手機 32A 原來對應的明文存取資料 PTA。根據處理器 36 本身解密出來的明文存取資料 PTA2 所記錄的網路狀態，手機 32A 就能進行驗證步驟；舉例來說，若明文存取資料 PTA2 中記錄手機 32A 之網路鎖為啟動，處理器 36 就會比對用戶識別卡 45 (見圖二) 中的用戶識別碼 46 是否符合明文存取資料 PTA2 中記錄之合法用戶識別碼。若符合，處理器 36 就會允許使用者進一步以手機 32A 存取通信網路 30 的通信服務。不論驗證步驟的結果如何，處理器 36 解密而得的明文存取資料 PTA2 都只會暫存於處理器 36 本身的揮發性記憶區中；等處理器 36 完成網路鎖的驗證步驟，也就可將明文存取資料 PTA2 釋放，不會暴露於手機 32A 的各個非揮發性的記憶體中 (像是資料記憶體 40A)。同理，當手機 32B 要進行驗證步驟時，手機 32B 也會以其防寫記憶體 50B 中的專屬解密金鑰 DKB 來將資料記憶體 40B 中的密文存取資料 CTB 解密，以取得對應的明文存取資料 PTB。



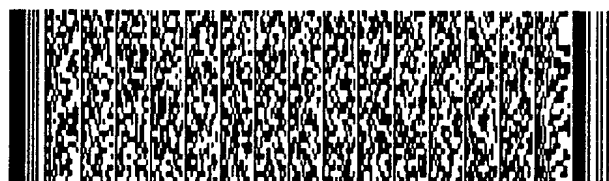
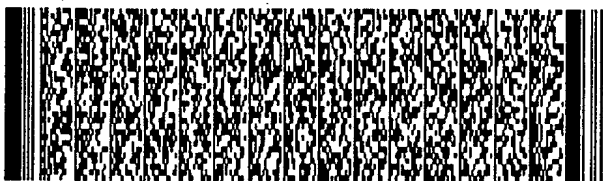
五、發明說明 (17)

本發明以上述的架構來實現網路鎖機制，就可有效保護網路鎖不被破解。如前面所討論過的，在習知技術中，非法使用者可將手機中儲存的網路鎖存取資料（也就是明文的存取資料）以破解存取資料覆蓋，或將其直接竄改，以使習知的手機在進行網路鎖之驗證步驟時，無法得知真正的網路鎖狀態。然而，在本發明中，上述方法都無法破解本發明的網路鎖機制。舉例來說，一意圖破解手機 32A 網路鎖之非法使用者可將手機 32B 中的密文存取資料 CTB 讀出並覆寫至手機 32A 中，以將手機 32A 原來的密文存取資料 CTA 用手機 32B 之密文存取資料 CTB 代替；但當手機 32A 要驗證網路鎖而根據解密金鑰 DKA 將資料記憶體 40A 中的密文存取資料 CTB 解密時，由於解密金鑰 DKA 對應的加密金鑰 EKA 並非加密密文存取資料 CTB 的加密金鑰 EKB，故處理器 36 不會解出正確的明文存取資料 PTB，其解密出來的明文存取資料 PTA2 會是沒有意義的，不具有明文存取資料的正確格式（舉例來說，正確明文資料必有一定欄位記錄網路鎖功能是否啟動）。當處理器 36 發現解密出來的明文存取資料 PTA2 沒有存取資料的正確格式而是無意義時，就可判斷手機 32A 之網路鎖已遭破壞。要以手機 32B 的密文存取資料 CTB 來破解（代替）手機 32A 原來的網路鎖，非法使用者必需要將手機 32A 中的解密金鑰 DKA 也覆寫為手機 32B 的解密金鑰 DKB，才能讓手機 32A 以手機 32B 的解密金鑰 DKB 將密文存取資料 CTB

五、發明說明 (18)

解密為具有正確格式的明文存取資料；然而，正如前面所強調的，手機 32A 中的解密金鑰 DKA 是儲存於防寫記憶體 50A 中，無法再被覆寫竄改，故非法使用者也無從破解本發明架構下的網路鎖。另外，若非法使用者直接竄改資料記憶體 40A 中的密文存取資料 CTA 而意圖破解手機 32A 的網路鎖，處理器 36 在驗證步驟中解密出來的明文存取資料 PTA2 勢必也會變成沒有意義的資料，不具有存取資料的正確格式；此時處理器 36 也可判斷手機 32A 的網路鎖遭到破壞。要破解手機 32A 的網路鎖機制，非法使用者要能將破解的明文存取資料（像是將網路鎖功能記錄為不動之存取資料）以加密金鑰 EKA 加密為破解的密文存取資料，再覆寫至手機 32A 中的資料記憶體；但是手機 32A 的加密金鑰 EKA 僅保留於通信網路 30 的網路服務端 48，並不會暴露於各手機中，且各手機中的解密金鑰並不等於對應的加密金鑰，故非法使用者將無法得出正確的破解密文存取資料，也就無法破解手機的網路鎖。

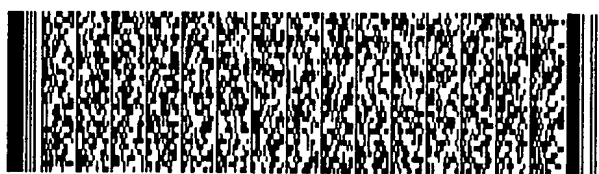
當手機 32A 的處理器 36 發現解密出來的明文存取資料 PTA2 沒有正確格式而判斷出網路鎖遭受破壞時，代表密文存取資料 CTA 已遭不明資料覆寫；此時處理器 36 可停止手機 32A 存取通信服務的功能，防止通信網路 30 的通信秩序及各方的合法權益遭受破壞。另外，在網路鎖受破壞時，處理器 32A 也可以用人機介面 41（於圖二）進一步提示手機 32A 的使用者需向服務提供端 48 確認其所應有的權



五、發明說明 (19)

益；而服務提供端 48 就可依據手機 32A 的裝置識別碼 IDA 於資料庫 52 中找出手機 32A 對應的加密金鑰 EKA，並依據此機加密金鑰 DKA，再以密碼演算法 54 將明文存取資料 PTA 加密為密文存取資料 CTA，並重新寫入至手機 32A 中的資料記憶體 40A，以恢復手機 32A 的網路鎖機制。當然，當處理器 36 發現網路鎖遭到破壞時，也可自動地透過通信網路 30 向服務提供端 48 提示其裝置識別碼 IDA，並要求服務提供端 48 透過通信網路將正確的密文存取資料 CTA 再度傳送至手機 32A，由處理器 40A 自動將其寫入資料記憶體 40A 中，以恢復手機 32A 對應的網路鎖機制。由於手機 32A 僅需密文資料 CTA 即可恢復網路鎖機制，即使透過無線通信網路傳輸密文存取資料 CTA，手機 32A 加解密金鑰也不會暴露於無線通信網路；此外，即使有非法使用者截獲此密文存取資料 CTA，因為各手機對應的解密金鑰皆相異，此密文存取資料 CTA 也無法用來破解其他手機（像是手機 32B）的網路鎖。尤其是當非法使用者以刪除密文存取資料 CTA 的手段意圖破解手機 32A 之網路鎖時，手機 32A 在找不到密文存取資料 CTA 的情形下，即可向服務提供端 48 要求再度傳輸密文存取資料 CTA，恢復原來的網路鎖機制，保護網路鎖不遭破解。

即使是正常網路鎖內容的改變，以本發明的架構，也可保護網路鎖的安全。舉例來說，若服務提供端 48 要主動改變手機 32A 的網路鎖內容（譬如說是將手機 32A 的



五、發明說明 (20)

網路鎖由啟動改變為不啟動)，網路服務端 48 可更新明文存取資料 PTA，再根據手機 32A 的加密金鑰 EKA 將更新後的明文存取資料 PTA 加密為新的密文存取資料 CTA。除了通知手機 32A 之使用者將手機 32A 攜至服務提供端 48，由服務提供端 48 (的相關技術人員) 將新的密文存取資料 CTA 寫入至手機 32A 外，服務提供端 48 也可透過無線通信網路 30 將新的密文存取資料 CTA 傳輸至手機 32A，由手機 32A 的處理器 36 將其寫入至資料記憶體 40A 中，代替原來的密文存取資料。這樣一來，不僅能方便手機 32A 的使用者，由於存取資料在通信網路上傳播時已經加密，也不擔心密文存取資料的暴露危害各手機的網路鎖安全。另外，在各手機的明文存取資料中，除了記錄對應手機的網路鎖狀態外，服務提供端還能另外再於明文存取資料中記錄該手機對應的裝置識別碼，使加密後的密文存取資料也隱含了該手機的裝置識別碼。當該手機進行認證步驟而將密文存取資料解密為明文存取資料後，除了依據明文存取資料是否有正確格式來判斷網路鎖是否遭破壞，也可比對解密出來的裝置識別碼及該手機真正的識別碼是否相符，以進行雙重檢查，判斷網路鎖機制是否遭到破壞。

總結來說，在習知技術中，由於網路鎖存取資料是以明文方式記錄於各手機中，易遭非法使用者以覆寫、直接竄改等方式加以破解，影響網路通信秩序及各方的



五、發明說明 (21)

合法權益。相較之下，本發明是對通信網路中的各手機分配一組獨一無二的加解密金鑰，網路服務端保留各手機對應的加密金鑰，以將各手機對應網路鎖之明文存取資料加密為對應的密文存取資料。而各手機僅保留密文存取資料，並以防寫、唯讀的方式記錄有對應的解密金鑰。當一手機要進行網路鎖之認證步驟時，係以該手機之解密金鑰將該密文存取資料解密為明文存取資料，再依據明文存取資料實現網路鎖機制。由於各手機的加解密金鑰不相同，即使非法使用者以其他手機的密文存取資料覆寫一手機的密文存取資料，該手機都會發現網路鎖遭破壞而中止對通信服務的非法存取，進而達到保護網路鎖機制的目的，維護通信網路的通信秩序及各方的合法權益。

以上所述僅為本發明之較佳實施例，凡依本發明申請專利範圍所做之均等變化與修飾，皆應屬本發明專利之涵蓋範圍。



圖式簡單說明

圖式之簡單說明

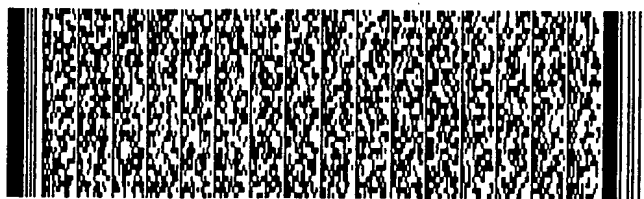
圖一為一習知通信網路中各手機及服務提供端相關配置的示意圖。

圖二為本發明通信網路中各手機及服務提供端相關配置的示意圖。

圖三為本發明網路鎖機制實施情形之示意圖。

圖式之符號說明

10、30	通信網路		
12-13、32A-32B		手機	
14、34	收發模組	16、36	處理器
18A、38A	麥克風	18B、38B	揚聲器
20、40A-40B			資料記憶體
21、41	人機介面	22	存取資料
23、IDA-IDB			裝置識別碼
24、45	用戶識別卡	26、46	用戶識別碼
28、48	服務提供端	29、49	基地台
50A-50B	防寫記憶體	52	資料庫
54	密碼演算法	EKA-EKB	加密金鑰
DKA-DKB	解密金鑰	PTA-PTB	明文存取資料
CTA-CTB	密文存取資料		



六、申請專利範圍

1. 一種使用於一通信網路的方法，用來識別該通信網路中一通信裝置是否可存取該通信網路的通信服務，其中該通信裝置包含有：

一資料記憶體，用來記錄一密文存取資料；以及
一防寫記憶體，用來以非揮發性的方式記錄一解密金鑰；

其中該防寫記憶體中記錄的資料不能被覆寫，使得即使該資料記憶體中記錄的資料被改變，該防寫記憶體中記錄之解密金鑰也不會被改變；

而該方法包含有：

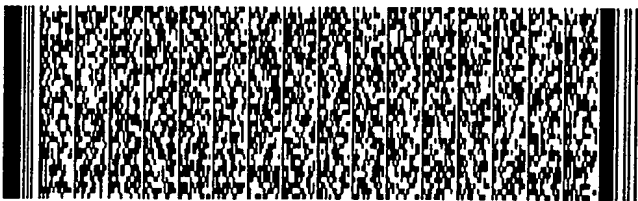
進行一驗證步驟，以讀取該防寫記憶體中之解密金鑰及讀取該資料記憶體中之密文存取資料；

再根據該解密金鑰，以一預設之密碼演算法將該密文存取資料解密為一明文存取資料，並根據該明文存取資料，判斷該通訊裝置是否可存取該通訊網路之通信服務。

2. 如申請專利範圍第1項之方法，其中該密碼演算法為一非對稱 (asymmetric) 之加解密演算法。

如申請專利範圍第1項之方法，其中該資料記憶體為一非揮發性的記憶體。

4. 如申請專利範圍第1項之方法，其另包含有：



六、申請專利範圍

根據一加密金鑰，將一對應該通信裝置的存取資料以該密碼演算法加密為該密文存取資料；其中該加密金鑰係對應於該解密金鑰，使得一明文在根據該加密金鑰以該密碼演算法加密為一密文後可根據該解密金鑰解密為原來之明文；以及
將該密文存取資料記錄至該資料記憶體。

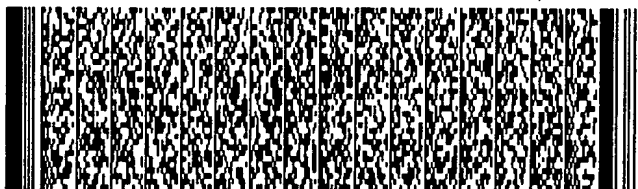
5. 如申請專利範圍第4項之方法，其另包含有：

在根據該加密金鑰加密出該密文存取資料前，根據該密碼演算法產生出該加密金鑰及該對應之解密金鑰。

6. 如申請專利範圍第4項之方法，其中該通信網路中另包含有一服務提供端，用來對該通信裝置提供通信服務；該服務提供端設有一資料庫，用來記錄該加密金鑰及對應該通信裝置的存取資料。

7. 如申請專利範圍第6項之方法，其中當根據該加密金鑰加密出該密文存取資料時，係於該服務提供端根據該資料庫中記錄之加密金鑰將對應該通信裝置的存取資料加密為該密文存取資料。

8. 如申請專利範圍第7項之方法，其中當要將該密文存取資料記錄至該資料記憶體時，係將該密文存取資料由該服務提供端透過該通信網路傳輸至該通信裝置，再以



六、申請專利範圍

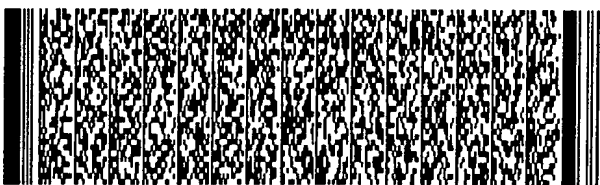
該通信裝置將該密文存取資料記錄至該資料記憶體。

9. 如申請專利範圍第4項之方法，其中該加密金鑰與該解密金鑰相異。

10. 如申請專利範圍第1項之方法，其中當根據該明文存取資料判斷該通信裝置是否可存取該通信網路之通信服務時，係根據該明文存取資料是否符合一預設存取資料來判斷；若該明文存取資料符合該預設存取資料，則判斷該通信裝置可存取該通信網路之通信服務。

11. 如申請專利範圍第1項之方法，其中該通信裝置中另包含有一用戶識別卡，用來記錄一用戶識別碼；而該明文存取資料中記錄有一預設識別碼；其中當根據該明文存取資料判斷該通信裝置是否可存取該通信網路之通信服務時，係根據該用戶識別碼是否符合該預設識別碼來判斷；若兩者符合，則判斷該通信裝置可存取該通信網路之通信服務；若否，則判斷該通信裝置不可存取該通信網路之通信服務，而該通信裝置會停止存取該通信網路。

12. 如申請專利範圍第1項之方法，其中該通信裝置為一手機，而該通信網路為一無線通信網路。



六、申請專利範圍

13. 一種用於一通信網路中的通信裝置，用來存取該通信網路的通信服務；該通信裝置包含有：

一資料記憶體，用來以非揮發性的方式記錄一密文存取資料；

一防寫記憶體，用來以非揮發性的方式記錄一解密金鑰；

其中該防寫記憶體中記錄的資料不能被覆寫，使得即使該資料記憶體中記錄的資料被改變，該防寫記憶體中記錄之解密金鑰也不會被改變；

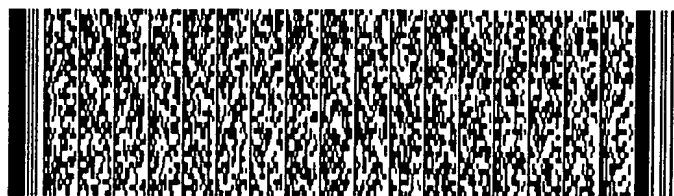
一處理器，用來控制該通信裝置的運作；

其中當該通信裝置要存取該通信網路之通信服務前，該處理器會進行一驗證步驟，以讀取該防寫記憶體中之解密金鑰及讀取該資料記憶體中之加密存取資料；

再根據該解密金鑰，以一預設之密碼演算法將該密文存取資料解密為一明文存取資料，並根據該明文存取資料，判斷該通訊裝置是否可存取該通訊網路之通信服務。

14. 如申請專利範圍第13項之通信裝置，其中該密碼演算法為一非對稱 (asymmetric) 之加解密演算法。

15. 如申請專利範圍第13項之通信裝置，其中該資料記憶體為一非揮發性的記憶體。



六、申請專利範圍

16. 如申請專利範圍第13項之通信裝置，其中該通信網路中另包含有一服務提供端，用來對該通信裝置提供通信服務；該服務提供端設有一資料庫，用來記錄一加密的金鑰及對應該通信裝置的存取資料；而該通信裝置中的密文存取資料係根據該加密金鑰，將對應該通信裝置的存取資料以該密碼演算法加密而得；其中該加密金鑰係對應該解密金鑰，使得一明文在根據該加密金鑰以該密碼演算法加密為一密文後可根據該解密金鑰解密為原來之明文。

17. 如申請專利範圍第16項之通信裝置，其中該加密金鑰及該對應之解密金鑰係根據該密碼演算法所計算出來的。

18. 如申請專利範圍第16項之通信裝置，其中將該密文存取資料係由該服務提供端透過該通信網路傳輸至該通信裝置，再由該處理器將該密文存取資料記錄至該資料記憶體。

19. 如申請專利範圍第13項之通信裝置，其中當該處理器根據該明文存取資料判斷該通信裝置是否可存取該通信網路之通信服務時，係根據該明文存取資料是否符合一預設存取資料來判斷；若該明文存取資料符合該預設存取資料，則該處理器會判斷該通信裝置可存取該通信



六、申請專利範圍

網路之通信服務。

20. 如申請專利範圍第13項之通信裝置，其中該通信裝置中另包含有一用戶識別卡，用來記錄一用戶識別碼；而該明文存取資料中記錄有一預設識別碼；其中當該處理器根據該明文存取資料判斷該通信裝置是否可存取該通信網路之通信服務時，係根據該用戶識別碼是否符合該預設識別碼來判斷；若兩者符合，則判斷該通信裝置可存取該通信網路之通信服務；若否，則判斷該通信裝置不可存取該通信網路之通信服務，而該通信裝置會停止存取該通信網路。

21. 如申請專利範圍第13項之通信裝置，其係為一手機，而該通信網路為一無線通信網路。

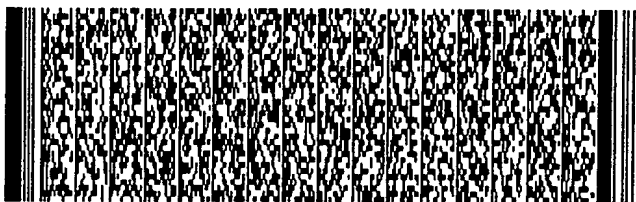
22. 一種使用於一通信網路的方法，其中該通信網路包含有：

複數個通信裝置，每一通信裝置包含有一防寫記憶體及一資料記憶體；

而該方法係用來驗證各通信裝置是否可存取該通信網路之通信服務；該方法包含有：

根據一密碼演算法，提供複數個相異的加密金鑰及複數個解密金鑰，其中各加密金鑰對應於一解密金鑰；

使得一明文在根據一加密金鑰以該密碼演算法加密



六、申請專利範圍

為一密文後可根據該加密金鑰對應之解密金鑰解密為原來之明文；

使不同的通信裝置對應於不同的加密金鑰；

將每一通信裝置對應的一筆存取資料根據該通信裝置對應之加密金鑰以該密碼演算法加密為一密文存取資料；

將對應每一通信裝置加密金鑰之解密金鑰記錄於該通信裝置中的防寫記憶體，以使該解密金鑰不會被覆寫；

將每一通信裝置的密文存取資料記錄於該通信裝置的資料記憶體；以及

當要驗證一通信裝置是否可存取該通信網路之通信服務時，根據該通信裝置防寫記憶體中之解密金鑰以該密碼演算法將該通信裝置資料記憶體中之密文存取資料解密，並根據解密後之密文存取資料來判斷該通信裝置是否可存取該通信網路之通信服務。

23. 如申請專利範圍第22項之方法，其中不同之加密金鑰對應之解密金鑰也互不相同。

24. 如申請專利範圍第22項之方法，其中該密碼演算法係一非對稱之加密演算法，使一加密金鑰與對應之解密金鑰不相等；而當一明文根據該加密金鑰以該密碼演算法加密為一密文後，該密文無法根據該加密金鑰以該

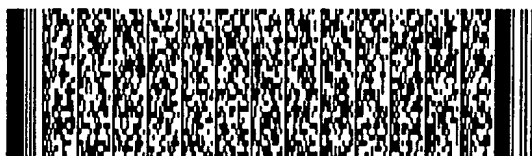
六、申請專利範圍

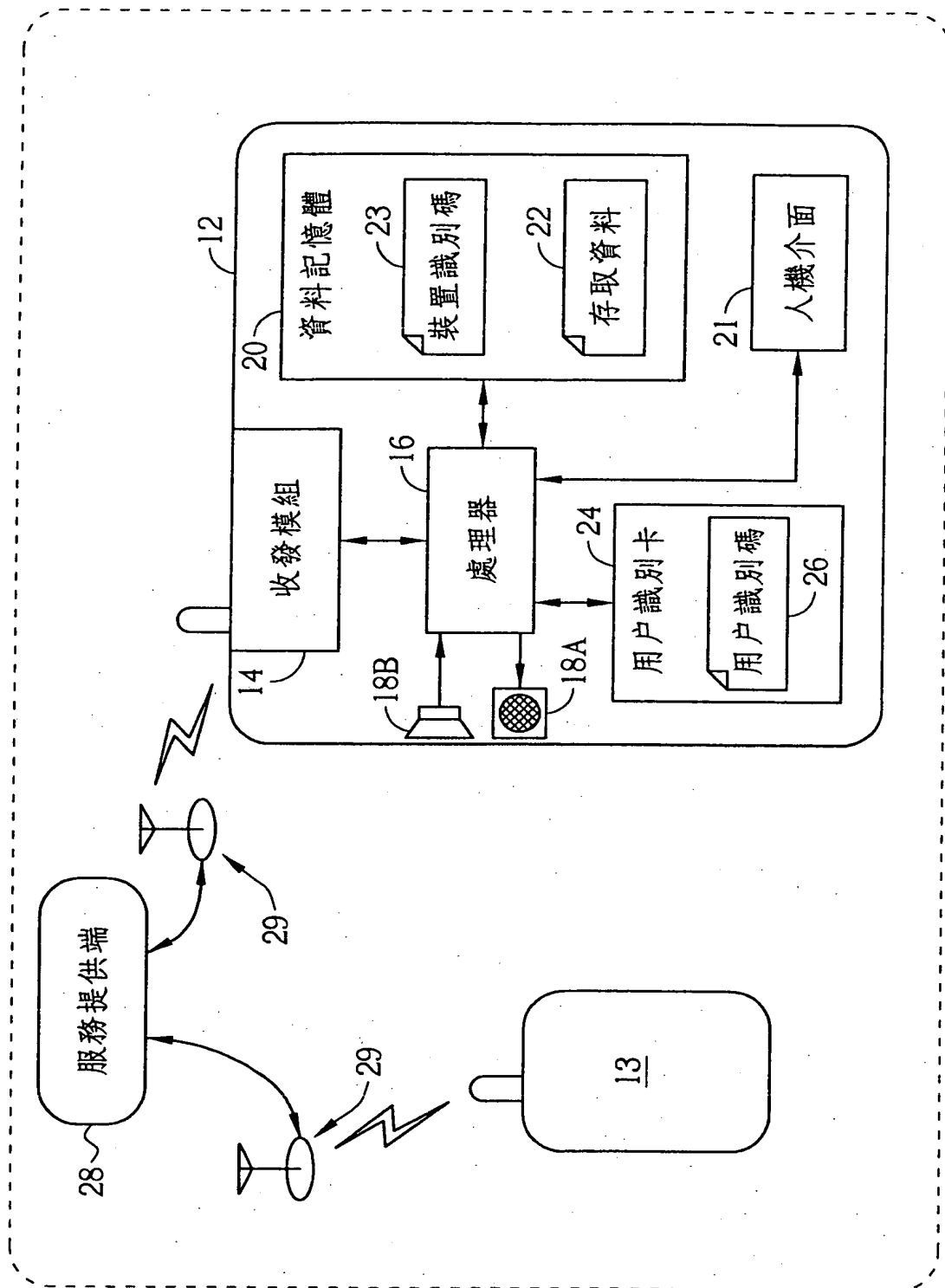
密碼演算法解密為原來之明文。

25. 如申請專利範圍第 22 項之方法，其中該通信網路另包含有一服務提供端，用來在各通信裝置間傳輸訊號以提供通信服務；該服務提供端設有一資料庫，而該方法另包含有：

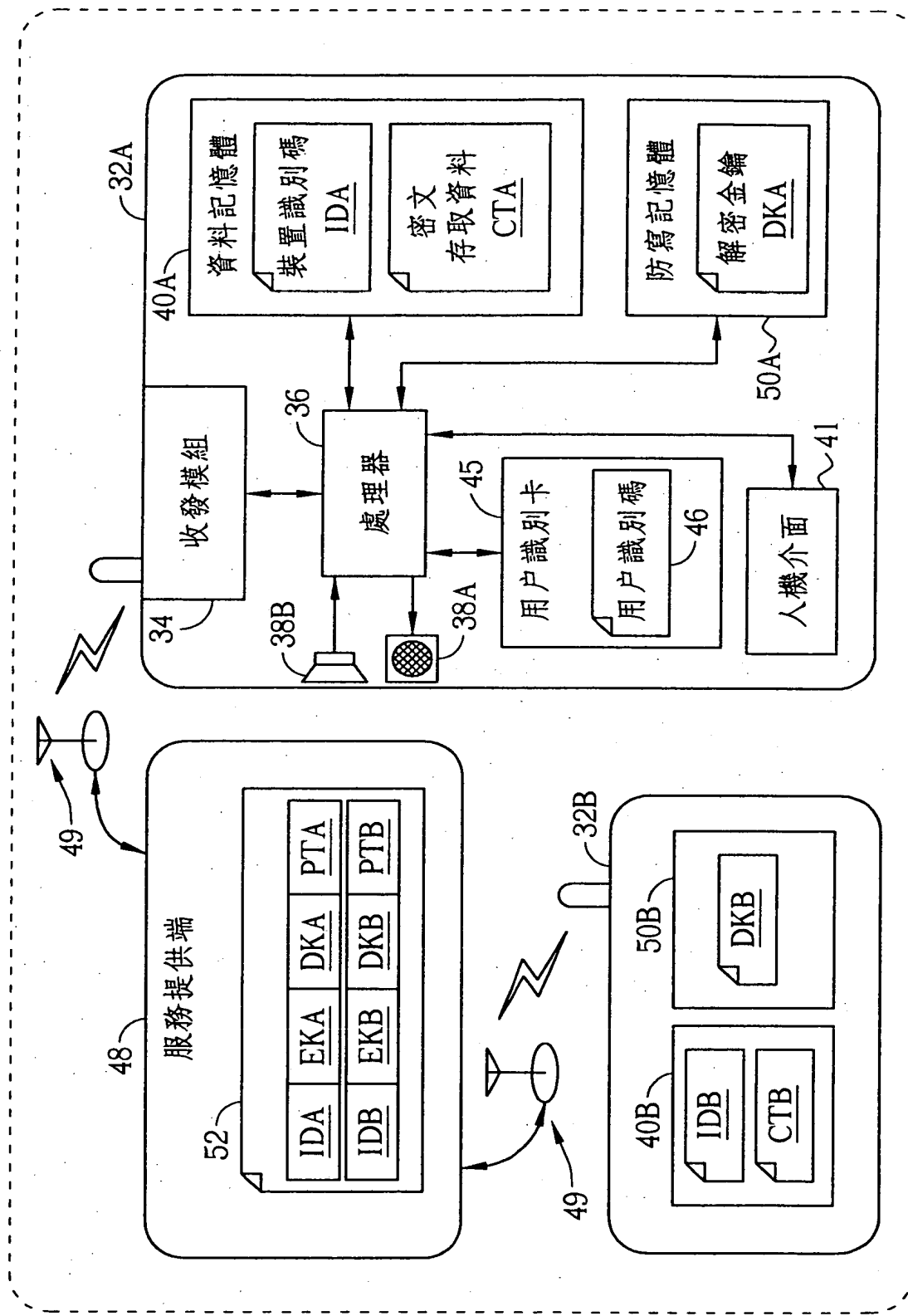
將各通信裝置對應之加密金鑰記錄於該資料庫中。

26. 如申請專利範圍第 22 項之方法，其中該等通信裝置為手機，而該通信網路為一無線通信網路。

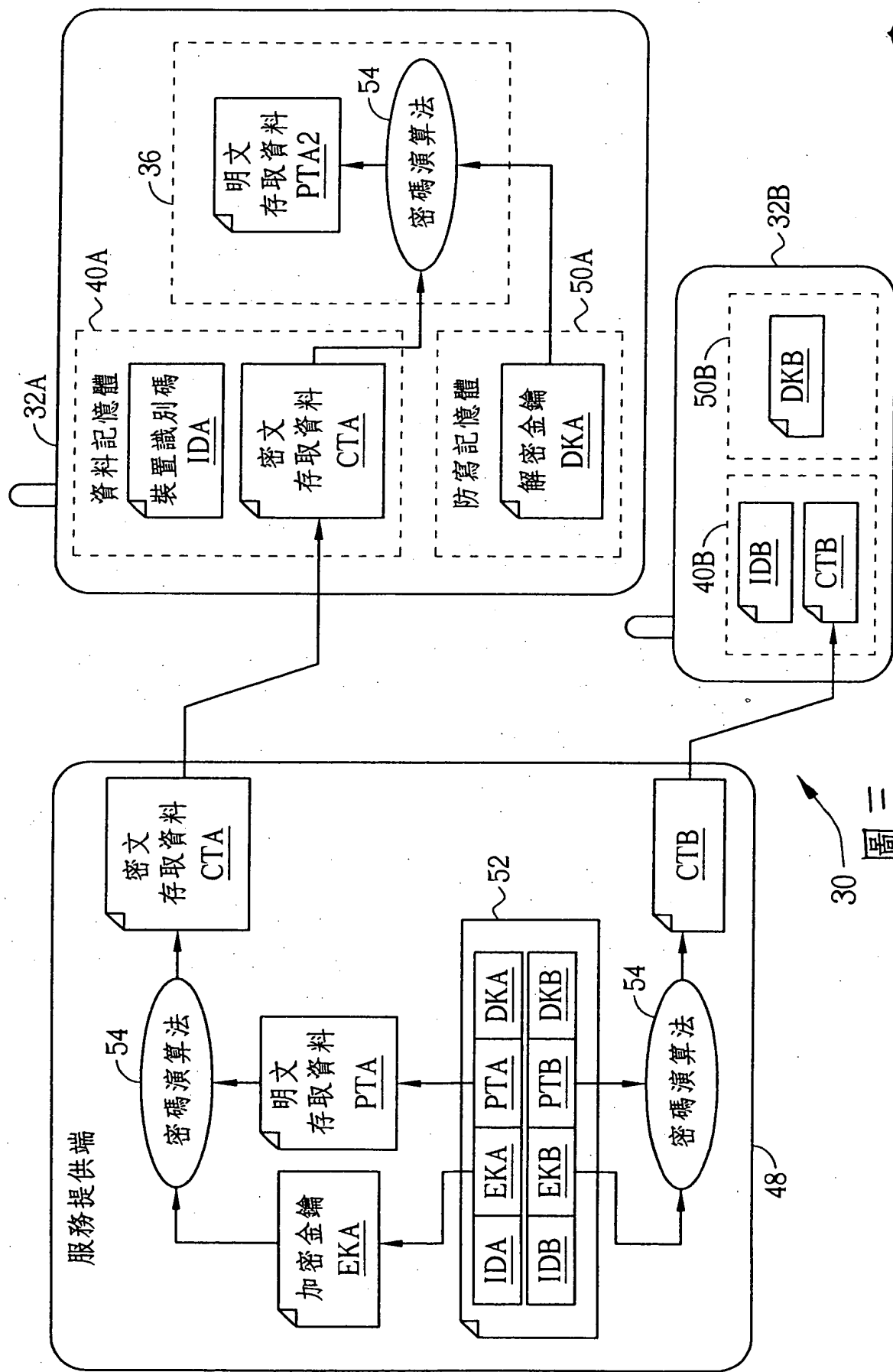




圖一



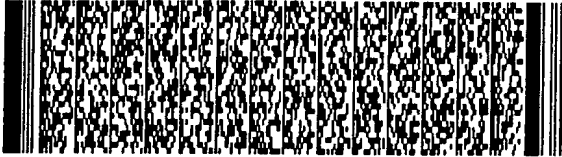
圖二



圖三

30

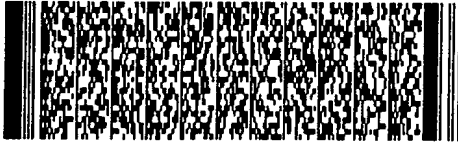
第 1/36 頁



第 1/36 頁



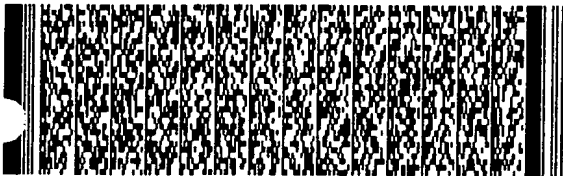
第 2/36 頁



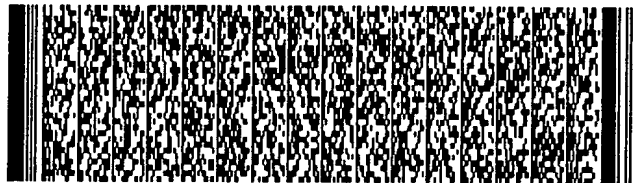
第 3/36 頁



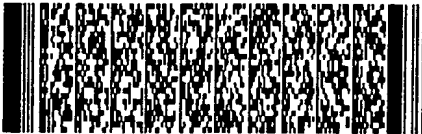
第 3/36 頁



第 4/36 頁



第 5/36 頁



第 6/36 頁



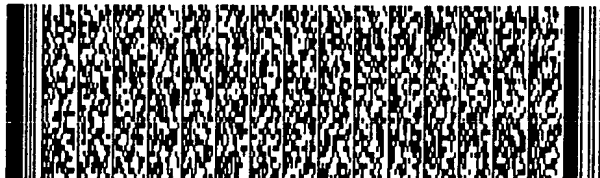
第 7/36 頁



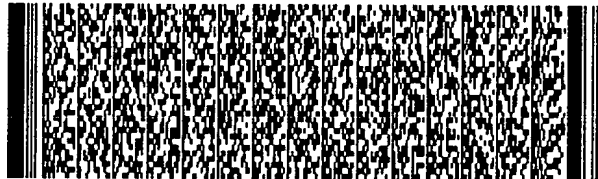
第 7/36 頁



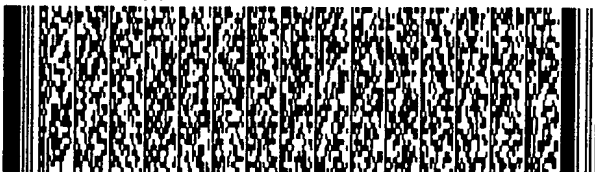
第 8/36 頁



第 8/36 頁



第 9/36 頁



第 9/36 頁



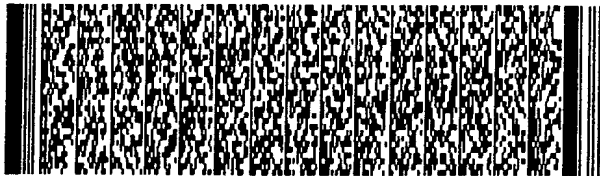
第 10/36 頁



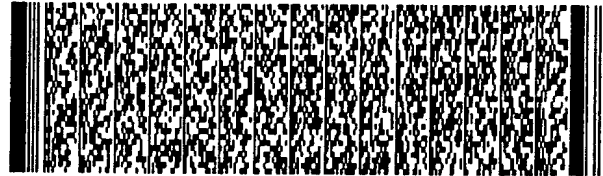
第 10/36 頁



第 11/36 頁



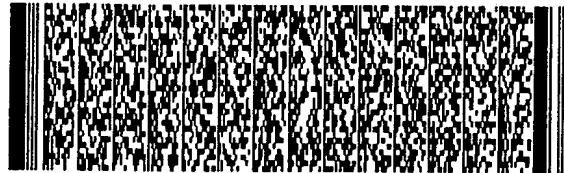
第 11/36 頁



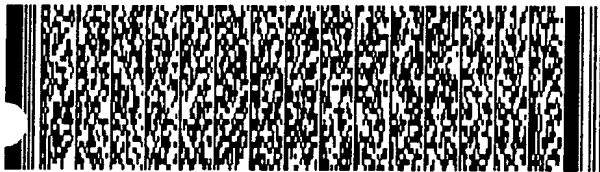
第 12/36 頁



第 12/36 頁



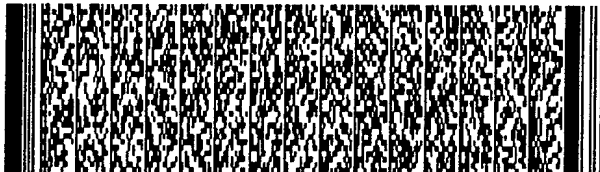
第 13/36 頁



第 13/36 頁



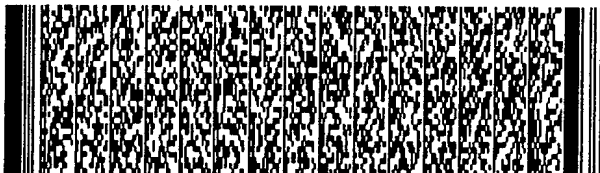
第 14/36 頁



第 14/36 頁



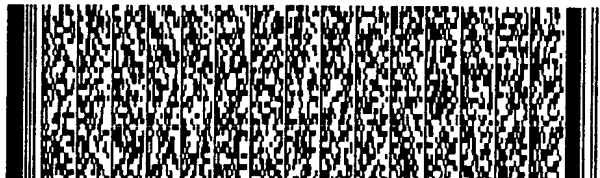
第 15/36 頁



第 15/36 頁



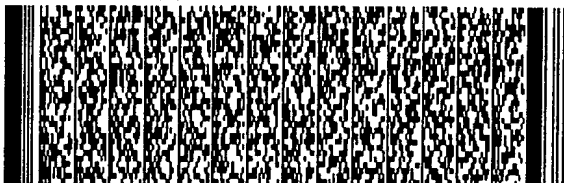
第 16/36 頁



第 16/36 頁



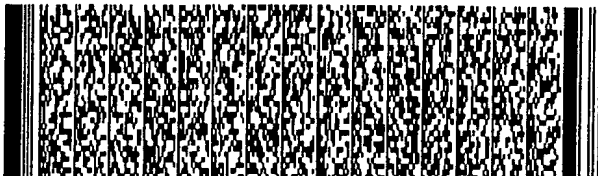
第 17/36 頁



第 17/36 頁



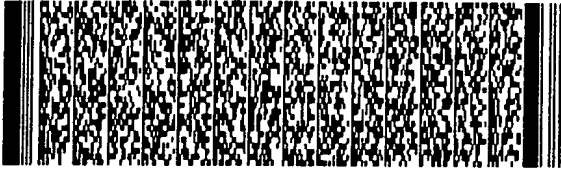
第 18/36 頁



第 18/36 頁



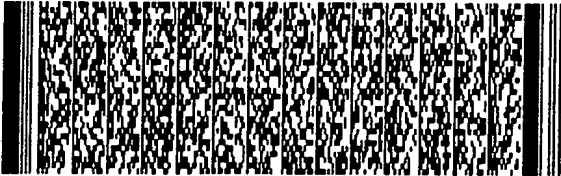
第 19/36 頁



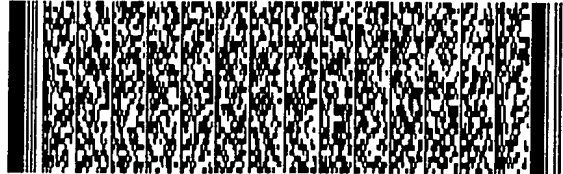
第 19/36 頁



第 20/36 頁



第 20/36 頁



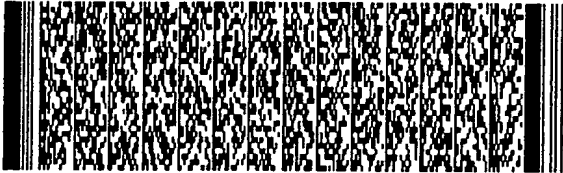
第 21/36 頁



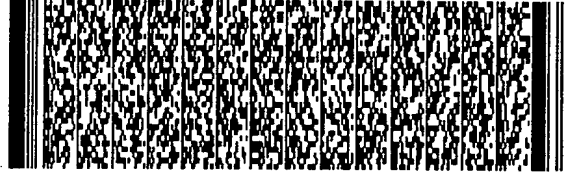
第 21/36 頁



第 22/36 頁



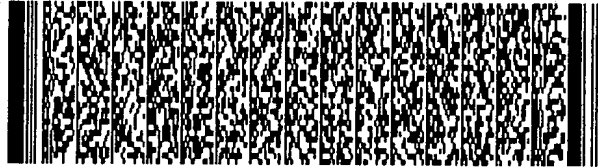
第 22/36 頁



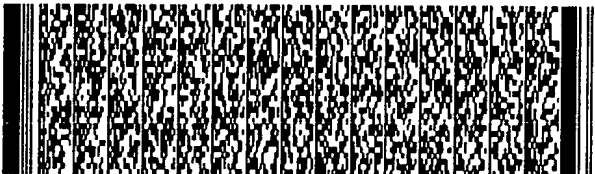
第 23/36 頁



第 23/36 頁



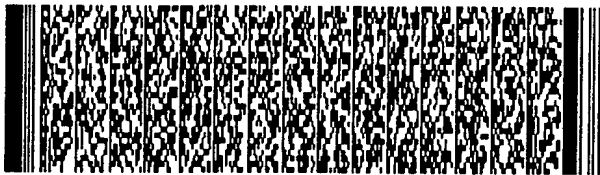
第 24/36 頁



第 24/36 頁



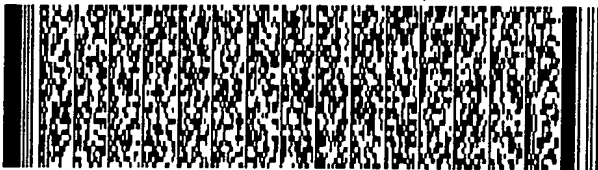
第 25/36 頁



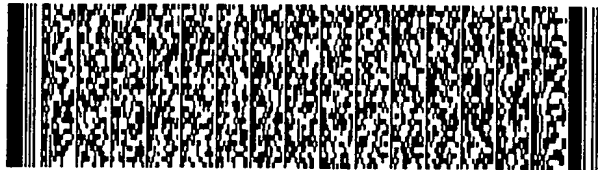
第 25/36 頁



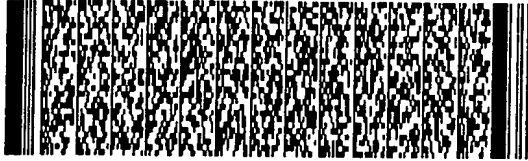
第 26/36 頁



第 26/36 頁



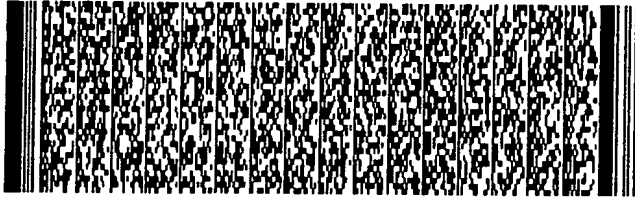
第 27/36 頁



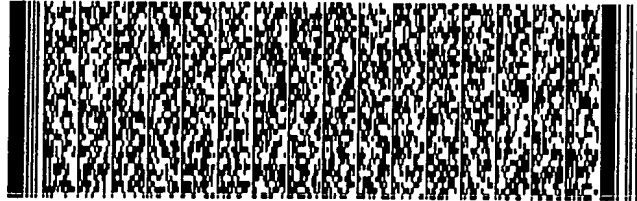
第 27/36 頁



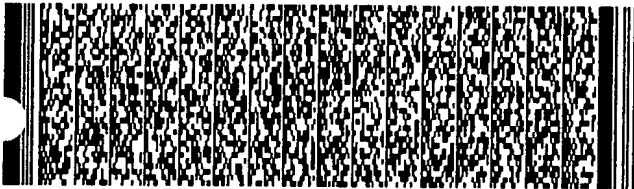
第 28/36 頁



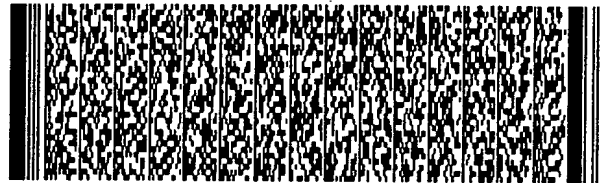
第 29/36 頁



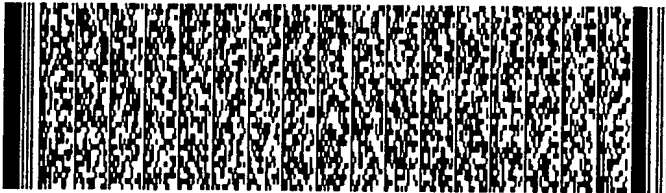
第 30/36 頁



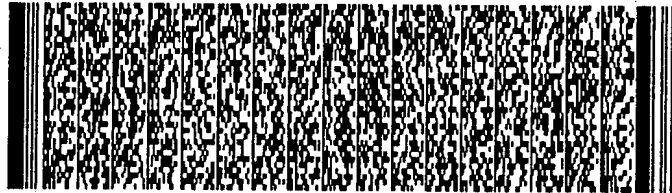
第 31/36 頁



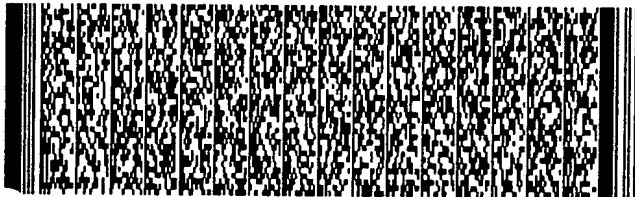
第 32/36 頁



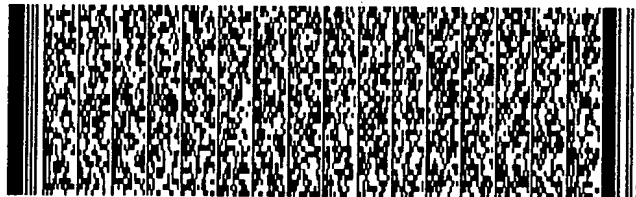
第 33/36 頁



第 34/36 頁



第 35/36 頁



第 36/36 頁

